## PIERWSZY KONTAKT

Podpisanie umowy o zachowaniu poufności (NDA)

Przedstawiciel managera sprzedaży i cyberbezpieczeństwa w Onwelo kontaktuje się z klientem w sprawie przyjętego w firmie podejścia i doświadczenia w zakresie testów penetracyjnych infrastruktury i aplikacji webowych.

Zanim nastąpi wymiana jakichkolwiek danych wrażliwych między firmą Onwelo a klientem, jeszcze na etapie wstępnych ustaleń należy podpisać umowę o zachowaniu poufności (NDA).

## OCENA ZAKRESU PRAC

Wymogi projektu

Zakres i cele audytu

W oparciu o wiedzę i dane przekazane przez klienta Onwelo opracowuje harmonogram testów penetracyjnych, ustala ich cele i przygotowuje scenariusze testowe w zgodzie z wymogami i oczekiwaniami zleceniodawcy.

Ustalenia na tym etapie pozwalają nam określić oczekiwania klienta, zidentyfikować jego aktualne bolączki i podnieść poziom usług w celu rozwiązania wszystkich problemów.

## USTALENIA KONTRAKTOWE

Wykaz prac

Start projektu

Po zatwierdzeniu celów, harmonogramu i kosztorysu projektu prowadzone są ustalenia kontraktowe i następuje oficjalny start projektu.

W oparciu o uzgodniony zakres prac i inne ustalenia Onwelo przystępuje do realizacji projektu. Na tym etapie klient udostępnia niezbędne informacje, takie jak dane uwierzytelniania, środowisko testowe itp.

## AUDYT

Przegląd procedur, polityk i infrastruktury

Rozmowy z kierownictwem i liderami

Audyt zabezpieczeń fizycznych w firmie*

Gromadzenie danych

Analiza danych

W zależności od celu i zakresu audytu zespół Onwelo przeprowadza szereg działań, takich jak analiza aktualnego stanu zabezpieczeń, gromadzenie danych i diagnoza ewentualnych zagrożeń i nieprawidłowości.

W oparciu o udostępnione polityki i procedury klienta Onwelo kontaktuje się z managerami i liderami wybranych zespołów, aby zgromadzić niezbędne dane i zidentyfikować ewentualne nieprawidłowości. Na życzenie klienta możemy również dokonać audytu stanu zabezpieczeń fizycznych w wybranej lokalizacji.

## TESTY

Skanowanie podatności*

Przegląd konfiguracji*

Dodatkowe skanowanie zabezpieczeń*

Po przeprowadzeniu audytu Onwelo oferuje również możliwość zlecenia analizy technicznej wybranego zakresu infrastruktury, która obejmuje skanowanie pod kątem podatności na zagrożenia i przegląd konfiguracji w celu oceny stanu odporności na zagrożenia, zabezpieczeń oraz innych ważnych aspektów utrzymania bezpieczeństwa.

Dodatkową wartość audytu stanowi skanowanie techniczne i analiza wybranego zakresu infrastruktury klienta, co pozwala na porównanie procedur i polityk z rzeczywistym stanem infrastruktury i procesów biznesowych.

## SPRAWOZDAWCZOŚĆ

Ocena ryzyka

Sprawozdanie

Na żądanie klienta przygotowujemy osobne wersje sprawozdania. Jedno jest przeznaczone dla zarządu i przedstawia wyniki na poziomie biznesowym. Drugie, o charakterze bardziej technicznym, trafia do zespołów informatycznych i zespołu rozwoju oprogramowania; zawiera wszystkie dane i rekomendacje niezbędne do podniesienia poziomu bezpieczeństwa wybranego zakresu infrastruktury.

Najważniejszą korzyścią każdego audytu jest pogłębione zrozumienie problemu, co pozwala na minimalizację lub całkowite usunięcie danego ryzyka w przyszłości. Po zakończeniu audytu Onwelo przedstawia złożone sprawozdanie z podsumowaniem przygotowanym specjalnie dla wybranych odbiorców po stronie klienta (zarząd, właściciele przedsiębiorstwa, zespoły techniczne itp.). W cytowanych sprawozdaniach zespół Cyber Security Onwelo przedstawia wyniki audytu, weryfikację koncepcji (PoC) oraz dalsze rekomendacje.

## PODSUMOWANIE

Prezentacja sprawozdania

Omówienie wyników

Omówienie rekomendacji

*usługa opcjonalna